IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

PHISHME, INC., Plaintiff, v. WOMBAT SECURITY TECHNOLOGIES, INC., Defendant.	Civil Action No. **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff PhishMe, Inc. ("PhishMe") brings this action for patent infringement against defendant Wombat Security Technologies, Inc. ("Wombat" or "Defendant") and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action for infringement of United States Patent No. 9,356,948 ("the '948 Patent"). The action arises under the laws of the United States related to patents, including 35 U.S.C. § 281.

2. The '948 Patent protects inventions used to detect and defend against phishing, a form of cyberattack. In a typical phishing attack, a computer user receives a malicious email disguised as though it were from a trusted source (*e.g.*, a co-worker, a bank, the IRS) that asks the user to perform an action, such as opening an email attachment or following an embedded link. When an unsuspecting user performs this action, malicious software is installed on the user's computer, for example, compromising the integrity not only of that computer, but of the

entire network to which the computer belongs. As described further below, phishing attacks have claimed millions of victims and have caused billions of dollars in damage.

THE PARTIES

3. PhishMe is a Delaware corporation. Its principal place of business is located at 1608 Village Market Boulevard, SE # 200, Leesburg, Virginia 20175.

4. Wombat is a Delaware corporation. On information and belief, Wombat's principal place of business is located at 3030 Penn Avenue, Suite 200, Pittsburgh, Pennsylvania 15201.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a). The Court has personal jurisdiction over Wombat because Wombat is a Delaware corporation established and existing under the laws of Delaware. The Court also has personal jurisdiction over Wombat because Wombat has continuously and systematically transacted business in this judicial district and, on information and belief, has committed acts of infringement in this district. Wombat has targeted Delaware residents with its infringing activities, including by employing an account executive responsible for marketing and sales of infringing products in Delaware. On information and belief, Wombat has offered for sale infringing products in this district and has induced others to perform the methods claimed in the '948 Patent in this district.

6. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c) and 1400(b) because Wombat is subject to personal jurisdiction in this district and, on information and belief, has committed acts of infringement in this district.

BACKGROUND

A. Phishing Poses A Significant Internet Threat To Organizations' Computing Systems

7. Computer systems have become a vital element of every organization. In particular, computer systems are increasingly being used to store enormous amounts of highly sensitive information, including business information, intellectual property, and state secrets.

8. As organizations' dependence on their computer systems has risen and as these systems are largely interconnected, the risks to those systems' integrity also have increased. One of the greatest threats to computer systems' integrity in the Internet age is known as "phishing." Phishing is a form of cyberattack in which a fraudulent email is disguised as a legitimate communication. A phishing email typically attempts to trick the recipient into responding, such as by clicking a link to a fraudulent webpage, downloading a malicious attachment, or directly providing sensitive information. A successful phishing attack compromises the recipient's computer system, or that of the recipient's organization, such as by giving the cyberattacker a foothold in the organization's computer network or by providing access to vital information, such as proprietary or personal data.

9. The impact of such phishing attacks is severe: they claim millions of victims and have caused billions of dollars in damage. Ammar Almomani, et al., *A Survey of Phishing Email Filtering Techniques*, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol. 15, pp. 2070-2090 (2013). For example, a form of cyberattack known as "Business Email Compromise" or "BEC" typically is initiated via phishing and caused losses totaling over $1.2 billion between October 2013 and August 2015. (https://www.ic3.gov/media/2015/150827-1.aspx#ref1; http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes.) In addition, ransomware attacks, a type of cyberattack in which malware prevents or limits access to a computer system until the victim pays a ransom,

often are initiated through phishing. (http://www.americanbar.org/content/dam/aba/administrative/cyberalert/ransomware.authcheckdam.pdf.) Earlier this year, a ransomware attack against Hollywood Presbyterian Medical Center disabled access to the hospital's electronic medical records system and other computer systems until the hospital paid a ransom equaling $17,000. (http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/.)

10. As shown above, phishing attacks have been waged against not only businesses' computer systems, but also against those of governmental and public service organizations, such as hospitals, schools, and police departments. (https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/; https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.) A cyberattack against the United States Office of Personnel Management, which has been called "the biggest government hack ever," was initiated via phishing. (http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.)

11. Phishing attacks also pose a significant threat to national security. In 2012, Defense Secretary Leon Panetta warned of a possible "cyber-Pearl Harbor" and noted that the United States has become increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks, and government. (http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.)

B. PhishMe's Patented Technology Protects Organizations And Improves Their Computing Systems' Security, Integrity, And Functionality

12. PhishMe is a pioneering company in assessing, combating, and preventing phishing and other cyberattacks. Launching its cybersecurity service publicly in 2008, PhishMe

has become the leading provider of threat management for organizations concerned about human susceptibility to advanced targeted attacks. PhishMe's success in securing its customers' computer systems against cyberattacks owes to its unique and innovative technology, which utilizes user-generated intelligence derived in near real-time to defend against the phishing threat.

13. A key element of PhishMe's computer technology is "Reporter™." Reporter™ is a software plug-in that improves upon existing phishing prevention systems by adding a user-interface that allows computer users to report suspicious emails to internal security teams or computer systems in a timely manner. The suspicious emails reported by users could be simulated phishing emails sent as part of a training campaign or potentially real phishing emails sent as part of an attack. Reporter™ enhances phishing detection and response systems by automatically distinguishing between these simulated and potentially real phishing emails, so that reports of possibly malicious emails are delivered to appropriate security operations and incident response teams. This saves significant computing resources and accelerates the detection of actual threats, and thus improves the overall security, integrity, and functionality of the organization's computing systems. Reporter™ also gives the end users immediate feedback when they report simulated phishing emails to reinforce and encourage their positive behavior. This allows organizations to leverage human intelligence to identify and detect phishing attacks, thereby preventing damage to computing systems and large-scale data breaches.

14. PhishMe has obtained numerous patents on its innovative cybersecurity technologies, including Reporter™. At the heart of this action is the '948 Patent. Titled "Collaborative Phishing Attack Detection," the '948 Patent issued on May 31, 2016, to Aaron

Higbee, Rohyt Belani, and Scott Greaux. PhishMe is the owner of all right, title and interest in and to the '948 Patent, a copy of which is attached as Exhibit A.

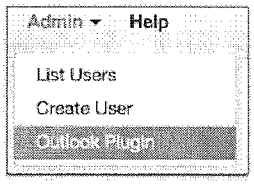
15. The '948 Patent covers systems and methods for assessing whether incoming emails are potentially phishing attacks and providing user training for distinguishing between malicious and benign emails. The specification discusses previous solutions to combating phishing attacks, such as "computer programs designed to detect and block phishing emails." ('948 Patent at 1:48-49.) It explains that these prior art solutions are insufficient because they cannot adapt to the dynamic nature of phishing attacks, as "phishing attack methods are constantly being modified by attackers to evade such forms of detection." (*Id.* at 1:49-51.) The invention claimed in the '948 Patent improves upon these prior art technologies. It utilizes notifications triggered by a user interface action that an email delivered to an individual user's email account is a possible phishing attack and uses the email's header to determine whether the possible phishing attack is a simulated phishing attack or potentially an actual, malicious phishing email. If the former, the patented invention provides feedback to the individual confirming that the identified email was a simulated phishing attack. If the latter, the patented invention sends the potential phishing email on, such as to a computer security technician for review, to an email address configured to receive the identified email, or to a computer configured to detect whether the identified email is a threat or real phishing attack. Some embodiments include a plug-in at an email client that provides a single graphical user interface action to be performed by the individual user that triggers the notification that a received email is a possible phishing attack.

C. Wombat's Products, Software, and Services

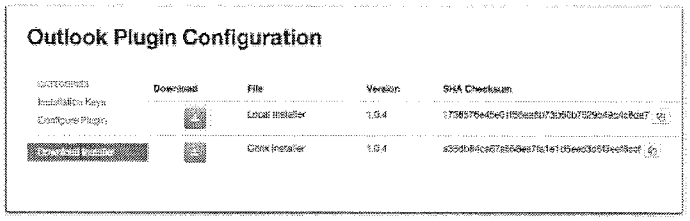
16. Wombat is a provider of cybersecurity products, including phishing awareness technology. In late 2015, Wombat acquired the company, ThreatSim, another provider of

phishing prevention technologies. Wombat subsequently has offered the ThreatSim product as part of its suite of cybersecurity offerings. Like PhishMe's patented Reporter™ technology, the ThreatSim product features a client-side plug-in that includes a user interface allowing the user to report a suspicious email as a possible phishing attack:

Within the ThreatSim portal click the Admin menu and select Outlook Plugin:



Download the ThreatSim for Outlook installer:



ThreatSim® for Outlook Administrator Guide

Also like PhishMe's patented Reporter™ technology, ThreatSim uses the email header to distinguish between a ThreatSim-created simulated phishing attack and a potential real, malicious phishing attack:

All ThreatSim emails contain a custom SMTP header that looks like this:

```
X-ThreatSim-Header: http://threatsim.com/speartraining?id=765fa3
X-ThreatSim-ID: 765fa3
```

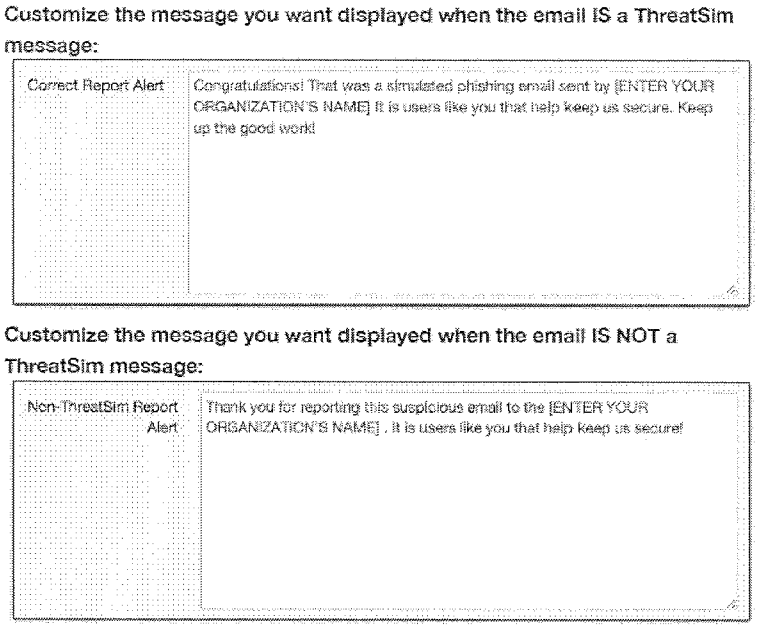
The X-ThreatSim-ID allows ThreatSim to identify which campaign and which user reported the email.

When the user clicks on the ThreatSim for Outlook button, Outlook will connect to our API at https://outlook.threatsim.com and send us the X-ThreatSim-ID. We then correlate the ID to the campaign and the target user, and mark the user as "Reported" within ThreatSim

If the X-ThreatSim-ID header is **not** found within the email, ThreatSim for Outlook forwards the email to the email address configured within your settings. The email is sent as a .eml attachment using the user's Outlook and is NOT sent to ThreatSim.

ThreatSim® for Outlook Administrator Guide

And once again like PhishMe's patented Reporter™ technology, if the identified email is a simulated phishing attack, ThreatSim provides user feedback. If not, the identified email is forwarded on to an identified email address for further analysis:



ThreatSim® for Outlook Administrator Guide

17. Wombat's Security Education Platform, which includes ThreatSim, PhishAlarm, and PhishAlarm Analyzer, is a suite of security awareness products, software, and services. Wombat makes, uses, sells, and offers for sale the products in its Security Education Platform in the United States.

COUNT I – PATENT INFRINGEMENT
(U.S. Patent No. 9,356,948)

18. PhishMe incorporates by reference and re-alleges Paragraphs 1–17 above as though fully restated herein.

19. Wombat has directly infringed the '948 Patent by making, using, selling, and offering for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '948 Patent in violation of 35 U.S.C. § 271(a).

20. In addition, Wombat has knowingly and intentionally induced infringement of the '948 Patent under 35 U.S.C. § 271(b) by actively encouraging others to make, use, sell, and offer for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '948 Patent. For example, Wombat has instructed and encouraged its customers to use its infringing products and software to perform the claimed methods of the '948 Patent, including through the following: (i) providing instructions and services to end users and customers of Wombat's products for using the products in their customary way; (ii) providing to third parties the products and software and related services that may be required for or associated with infringement of the '948 Patent; (iii) selling and offering to sell Wombat's infringing products in the United States; and (iv) promoting the infringing products on Wombat's website. On information and belief, Wombat has undertaken the above actions with knowledge that the induced acts infringe one or more claims of the '948 Patent, or Wombat subjectively believes that there is a high likelihood that the induced acts infringe the '948 Patent and it has taken deliberate steps to avoid learning that the induced acts do infringe the '948 Patent.

21. Further, Wombat has contributed to the infringement of the '948 Patent under 35 U.S.C. § 271(c) by selling and offering for sale, without license or authority, the infringing products and software in the United States, knowing that such products and software are especially made or adapted for use in infringement of the '948 Patent, are not a staple article or commodity of commerce suitable for any substantial non-infringing use, and that others, such as Wombat's customers and end-users, use such products and software to infringe the '948 Patent.

22. Wombat has had knowledge of the '948 Patent and the infringing nature of its activities since no later than May 31, 2016, when it received a letter from PhishMe identifying the '948 Patent and discussing Wombat's acts of infringement. Wombat also has had knowledge of PhishMe's cybersecurity inventions, including those described in the '948 Patent, as early as August 21, 2015, when Wombat cited a U.S. Patent No. 8,719,940, which is related to the '948 Patent, as prior art during prosecution of Wombat's U.S. Patent No. 9,280,070. Finally, Wombat has had knowledge of the '948 Patent and that its actions and products, software, and services infringe that patent as of the filing of this complaint. Despite knowing that it is infringing the '948 Patent, Wombat has continued to make, use, sell, and offer for sale its infringing products, software, and services and to actively encourage others to use its infringing products, software, and services to perform the '948 Patent's claimed methods.

23. PhishMe has been and continues to be damaged by Wombat's infringement of the '948 Patent in an amount to be determined and subject to proof at trial. In addition, Wombat's infringement of the '948 Patent has irreparably harmed PhishMe. For example, Wombat has used and currently is using PhishMe's patented inventions to compete against PhishMe.

JURY DEMAND

24. PhishMe demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to Fed. R. Civ. P. 38 and D. Del. LR 38.1.

PRAYER FOR RELIEF

WHEREFORE, PhishMe respectfully requests that this Court enter judgment in its favor as follows:

A. Declare that Wombat has infringed the '948 Patent, either literally or under the doctrine of equivalents;

B. Declare that Wombat has induced infringement of the '948 Patent;

C. Declare that Wombat has contributed to the infringement of the '948 Patent;

D. Award PhishMe past and future damages, together with prejudgment and post-judgment interest, to compensate for Wombat's infringement of the '948 Patent in accordance with 35 U.S.C. § 284;

E. Declare that this case is exceptional under 35 U.S.C. § 285;

F. Award PhishMe its costs and attorneys' fees under 35 U.S.C. § 285;

G. Issue an injunction barring Wombat and its officers, directors, agents, employees, affiliates, attorneys, and all others acting in privity or in concert with it, and its parents, subsidiaries, divisions, successors, and assigns, from further acts of infringement of the '948 Patent; and

H. Grant PhishMe such other and further relief as the case may require and the Court may deem just and proper under the circumstances.

YOUNG CONAWAY STARGATT & TAYLOR, LLP

Anne Shea Gaza

Anne Shea Gaza (No. 4093)
Samantha Wilson (No. 5816)
Rodney Square
1000 North King Street
Wilmington, DE 19801
(302) 571-6600
agaza@ycst.com
swilson@ycst.com

Attorneys for Plaintiff PhishMe, Inc.

OF COUNSEL:

MORRISON & FOERSTER LLP
Hector G. Gallegos
Joshua A. Hartman
Fahd H. Patel
2000 Pennsylvania Ave., NW
Washington, DC 20006-1888
(202) 887-1500

MORRISON & FOERSTER LLP
Mehran Arjomand
707 Wilshire Boulevard
Los Angeles, California 90017-3543
(213) 892-5200

Dated: June 1, 2016